REDACTED

Federal Housing Finance Agency
Office of Inspector General

Despite FHFA's Acknowledgement that Enterprise Reliance on Third-Parties Represents a Significant Operational Risk, No Targeted Examinations of Fannie Mae's Third-Party Risk Management Program Were Completed Over a Seven-Year Period

This report contains redactions of information that is privileged or otherwise protected from disclosure under applicable law.

Audit Report • AUD-2021-007 • March 29, 2021

AUD-2021-007

March 29, 2021

Executive Summary

The Federal Housing Finance Agency (FHFA) is charged by the Housing and Economic Recovery Act of 2008 with the supervision of Fannie Mae and Freddie Mac (together, the Enterprises), any affiliate of the Enterprises, and the Federal Home Loan Banks (collectively, the regulated entities). Its mission as a federal financial regulator includes ensuring the safety and soundness of its regulated entities so that they serve as a reliable source of liquidity and funding for housing finance and community investment. FHFA has also served as conservator of the Enterprises since 2008.

FHFA maintains that it uses a risk-based approach to supervisory examinations, prioritizing examination activities based on the assessed risk of a given practice to a regulated entity's safe and sound operation or to its compliance with applicable laws and regulations. Within FHFA, the Division of Enterprise Regulation (DER) is responsible for supervision of the Enterprises. Pursuant to FHFA's announced risk-based approach to supervision, DER conducts targeted examinations and ongoing monitoring.

Under the supervisory framework established by DER, ongoing monitoring is used to analyze information and identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention. Targeted examinations complement ongoing monitoring: they enable examiners to conduct "a deep or comprehensive assessment" of selected areas found to be of high importance or risk. Because each of these examination activities has a separate purpose, they are not interchangeable.

A third-party provider relationship is a business arrangement between a regulated entity and another entity that provides a product or service. Regulated entities use third-party providers in their operations to reduce costs, enhance performance, and obtain access to specific expertise, applications, and systems. Both Fannie Mae and DER acknowledge that Fannie Mae's use and reliance on third-party relationships present a significant risk. Effective risk management of third-party provider relationships is essential to the safe and sound operations of the regulated entities.

We conducted this audit to determine what examination activities DER completed, during the period 2014 through December 31, 2020, in response to identified risks in Fannie Mae's management of third-party provider relationships with vendors that provide operational support and information technology services, such as vendors that supply products, information, and services (e.g., audit and accounting services, telecommunications, data, cloud computing, information security). (FHFA's oversight of Enterprise

AUD-2021-007

March 29, 2021

supervision over seller/servicers, another type of third-party provider, was not included in the scope of this audit.)

DER records show that DER's last completed targeted examination of Fannie Mae's third-party risk management (TPRM) program was during the 2013 examination cycle. DER issued [redacted] Matters Requiring Attention (MRAs) from this targeted examination. For [redacted] of those MRAs, Fannie Mae took more than six years to address the deficiency that gave rise to it. In light of the express recognition by DER and Fannie Mae of the established [redacted] risk associated with management of these third party providers and the more than six years that Fannie Mae took to remediate this MRA, DER's governing supervisory framework warranted the completion of one or more targeted examinations of this risk during this period. No targeted examinations were completed from 2014 through 2020. During 2014 through 2020, DER examination records reflect that DER's completed examination activities related to Fannie Mae's TPRM program consisted solely of ongoing monitoring activities.

We also assessed in this audit whether FHFA followed its standards when performing the ongoing monitoring activity (and three ongoing monitoring activities to assess the sufficiency of MRA remediation), which were completed during 2019 and 2020. We found that the ongoing monitoring activities that DER completed during this period complied with applicable examination guidance.

We make one recommendation to address our finding. In a written management response, FHFA agreed with our recommendation.

This report was prepared by James Lisle, Audit Director; Marco Uribe, Auditor-in-Charge; and Christopher Mattocks, Auditor; with assistance from Abdil Salah, Assistant Inspector General of Audits, and Bob Taylor, Senior Advisor. We appreciate the cooperation of FHFA staff, as well as the assistance of those who contributed to the preparation of this report.

The report has been distributed to Congress, the Office of Management and Budget, and others, and will be posted to our website, www.fhfaoig.gov, and www.oversight.gov.

Marla A. Freedman, Senior Audit Executive /s/

TABLE OF CONTENTS

ABBREVIATIONS

AB 2018-08	Advisory Bulletin, *Oversight of Third-Party Provider Relationships*
CSS	Common Securitization Solutions, LLC
DER	Division of Enterprise Regulation
EIC	Examiner-in-Charge
Enterprises	Fannie Mae and Freddie Mac
Fannie Mae	Federal National Mortgage Association
FHFA	Federal Housing Finance Agency
Freddie Mac	Federal Home Loan Mortgage Corporation
MRA	Matter Requiring Attention
OIG	Federal Housing Finance Agency Office of Inspector General
OPB	Operating Procedures Bulletin
TPRM	Third-Party Risk Management

BACKGROUND

Fannie Mae and FHFA Have Identified Third-Party Providers as a Significant Operational Risk

Fannie Mae, in its 2019 Annual Report on Form 10-K, reported that reliance on third-party providers presents a significant operational risk and a failure in the operational systems or infrastructure of third-parties in which it does business could materially adversely affect its business, impair liquidity, cause financial loss, and harm reputation. DER, in its 2019 and 2020 Risk Assessments of Fannie Mae, echoed that view:[1] It rated the risk to the Enterprises from third-party providers as [redacted].[2]

FHFA Lacks Statutory Authority to Examine Third-Party Providers; It Has Communicated to the Enterprises its Expectations of Their Oversight of those Providers and Examines the Enterprises to Ensure that Their Oversight Is Sufficient

FHFA lacks statutory authority to examine third-party providers.[3] To meet the critical need for Enterprise oversight of third parties, FHFA issued several advisory bulletins communicating its supervisory expectations.

One of those bulletins is Advisory Bulletin 2018-08, *Oversight of Third-Party Provider Relationships* (AB 2018-08).[4] That Advisory Bulletin provides guidance to the regulated entities on assessing and managing risks associated with third-party provider relationships. In

[1] In its 2019 Risk Assessment, DER stated that the Enterprise's inherent third-party provider relationship risk is [redacted], due to the [redacted] at Fannie Mae that are [redacted]. This included vendors that supply cloud services, information technology systems, and enterprise-wide applications. Similarly, DER's 2020 Risk Assessment rated third-party provider relationship risk as [redacted], noting that "The [redacted] or the [redacted] Fannie Mae's [redacted] Enterprise to [redacted]."

[2] In light of the risks with the Enterprises' use of third-party providers, OIG published two white papers during 2020 related to these risks: *Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection* (Mar. 12, 2020) (WPR-2020-003) (online ***here***), which described the Enterprises' third-party risk management programs as they pertain to assessing and selecting one particular type of third-party – financial technology companies; and *Enterprise Monitoring of Cloud Computing Service Provider* (Aug. 12, 2020) (WPR-2020-005) (online ***here***), which described the Enterprises' monitoring procedures for third-party cloud service providers, pursuant to FHFA guidance.

[3] FHFA requested this authority in its annual report to Congress. FHFA, *2019 FHFA Report to Congress*, at 15 (June 15, 2020) (available on the FHFA website ***here***).

[4] AB 2018-08 is available on the FHFA website ***here***.

it, FHFA set forth its expectation that each regulated entity establish and maintain a TPRM program that includes the following:

- Governance – (a) policies and practices regarding the responsibilities of the board and senior management; (b) other policies, procedures, and internal standards; and (c) reporting.

- Risk Management Phases – assessment of the rigor of the risk management program of each third-party provider, including five phases: (a) risk assessment, (b) due diligence in third-party provider selection, (c) contract negotiation, (d) ongoing monitoring, and (e) termination.

To assess whether the Enterprises' oversight of third-party providers is safe and sound, DER conducts examination activities for Enterprise oversight activities. Pursuant to its announced risk-based approach to supervision which prioritizes examination activities based on the risk to the Enterprises' safe and sound operation or to its compliance with applicable laws and regulations, DER conducts targeted examinations and ongoing monitoring. Ongoing monitoring is performed to analyze information and to identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention. Targeted examinations complement ongoing monitoring: they enable examiners to conduct "a deep or comprehensive assessment" of selected areas found to be of high importance or risk.[5] FHFA's annual examination plans identify the examination activities, both ongoing monitoring and targeted examinations, expected to be completed during that examination cycle.

FHFA's Examination Manual Provides Guidance for Examiners to Assess Risks Associated with Third-Party Provider Relationships

FHFA provides guidance to DER teams performing examinations of the Enterprise's third-party risk management through a module in DER's Enterprise Examination Manual, Oversight of Third-Party Provider Relationships, issued in 2020.[6] This module is consistent with the supervisory expectations outlined in AB 2018-08 and serves as a resource for DER examiners to understand, evaluate, and assess risks associated with the Enterprises' third-party provider relationships.

[5] In a technical comment to a draft of this report, FHFA highlighted examination guidance issued by DER in February 2020 that revised the definitions of examination activities. That guidance was issued after the examination activities that are the focus of this audit were planned. For those reasons, FHFA's reliance on these revised definitions is unavailing.

[6] DER's examination modules provide background information on Enterprise operations and the regulatory environment (applicable laws, regulations, and examination guidance) relating to specific topics, as well as examination work programs that provide procedures that examiners are expected to consider when conducting examinations relating to these topics.

FACTS AND ANALYSIS

DER's Planned and Completed Examination Activities Related to Third-Party Provider Relationships From 2014 Through 2020 Consisted Solely of Ongoing Monitoring Activities, Notwithstanding the Known Significant Operational Risk Associated with These Relationships

As discussed, Fannie Mae has publicly disclosed that reliance on third-party providers presents a significant operational risk and a failure in the operational systems or infrastructure of third-parties in which it does business could materially adversely affect its business, impair liquidity, cause financial loss, and harm reputation. It did not limit its assessment only to third-party seller/servicers: it cautioned that its reliance on all types of third-party providers presents a significant operational risk. DER has underscored that risk and rated the risk to the Enterprises from third-party providers as [redacted].

Under the supervisory framework established by DER, ongoing monitoring is used to analyze information and identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention. Targeted examinations complement ongoing monitoring: they enable examiners to conduct "a deep or comprehensive assessment" of selected areas found to be of high importance or risk. Because each of these examination activities has a separate purpose, they are not interchangeable.

Given that both Fannie Mae and DER recognize the established, high operational risk from third-party providers, that identified significant high risk should drive DER to plan targeted examinations to conduct "deep or comprehensive" assessments, pursuant to its examination guidance. However, DER records show that, for the years 2013 through 2020, DER's last completed targeted examination of Fannie Mae's TPRM program was during 2013. This targeted examination resulted in [redacted] MRAs: [redacted] Fannie Mae must [redacted] Fannie Mae must [redacted], and [redacted] Fannie Mae must [redacted]. These [redacted] MRAs were closed in [redacted], respectively. DER planned a targeted examination for the 2014 examination cycle to assess expenses and controls around information technology vendors but it was put on hold. We found no evidence that it was performed in subsequent years. DER also planned a targeted examination for the 2017 examination cycle to assess the effectiveness of Fannie Mae's new TPRM monitoring program. A mid-year update to the 2017 examination plan reported a delay in this targeted examination: "Significant revisions are currently being made to TPRM Standards [by Fannie Mae], which need to be in place before this exam

commences." According to DER documentation, this targeted examination was converted into part of a 2018 ongoing monitoring activity that was completed in January 2019.

DER records show that DER planned five ongoing monitoring activities during 2019 and 2020. Of these five, three were conducted to determine the progress of Fannie Mae's remediation of outstanding MRAs related to deficiencies in its TPRM framework, all of which were completed, as discussed above. Of the other two planned for Fannie Mae's TPRM program, a known high risk to Fannie Mae, only one was completed.

DER's examination managers for Fannie Mae explained that examiners were comfortable with these two planned ongoing monitoring activities because DER had previously examined Fannie Mae's TPRM program (in 2013 and 2017) and had issued [redacted] MRAs. In addition to the [redacted] MRAs issued in connection with the 2013 targeted examination, DER records show that DER issued [redacted] MRAs arising from deficiencies in Fannie Mae's [redacted], identified through an ongoing monitoring activity in 2017. [redacted] MRA required Fannie Mae to [redacted] and to [redacted]. The [redacted] MRA required Fannie Mae's Enterprise Risk Management function to [redacted] Fannie Mae's [redacted].

According to DER records, the 2017 ongoing monitoring activity (and the [redacted] MRAs issued from it) occurred after Fannie Mae enhanced and/or developed new policies, procedures, and processes to manage third-party risk in response to these MRAs, which examiners had monitored. Notwithstanding these deficiencies identified by DER from this activity, examination managers reported to us that, during development of the 2019 examination plan, they did not have a specific issue or concern that warranted a targeted examination in the area of third-party vendors. DER examination managers reported to us that they were comfortable with planning only two ongoing monitoring activities involving the operational risk posed by third-party vendor relationships during the 2019 and 2020 examination cycles. Of these two planned monitoring activities, only one was completed from 2019 through 2020.[7]

In a technical comment to a draft of this report, DER acknowledged that targeted examinations can be more comprehensive than monitoring activities but asserted that it followed a "strategic approach" when conducting ongoing monitoring of Fannie Mae's implementation of a comprehensive enterprise-wide TPRM framework. It maintained that this approach took into appropriate consideration both the evolving nature of the framework and

[7] These examiners also pointed to a targeted examination of Fannie Mae's cloud security controls review that was commenced in response to information gained during DER's ongoing monitoring activities and completed in January 2021. Supervisory correspondence for this targeted examination reported [redacted] MRA and [redacted] other adverse examination findings.

management's implementation of the framework in Fannie Mae's business lines and the outstanding MRAs from 2013. According to DER, the classification of the examination work as an ongoing monitoring activity had no bearing on the comprehensiveness of the work performed and/or documentation of the work.[8]

Whatever the strategic approach of the assigned examiners, they are required to follow the applicable supervisory framework established by FHFA and DER. That framework directed that ongoing monitoring would be used to analyze information and identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention. As envisioned by this framework, targeted examinations complement ongoing monitoring: they enable examiners to conduct "a deep or comprehensive assessment" of selected areas found to be of high importance or risk. Given the known [redacted] risk associated with third-party provider relationships and the more than six years that Fannie Mae took to remediate the 2013 MRA on [redacted], application of DER's supervisory framework should have caused DER to schedule and conduct targeted examinations of Fannie Mae's TPRM program to provide "deep or comprehensive assessment[s]," along with ongoing monitoring. While we understand the need for examiners to have flexibility in the type of examination activities they schedule and conduct, in our view, applicable guidance should have caused DER to plan and complete one, if not more, targeted examinations over a seven-year period of Fannie Mae's TPRM program in light of its acknowledged high risk.

Review of Examiner Documentation Found that FHFA Followed its Standards in Conducting the One Ongoing Monitoring Activity Related to Fannie Mae's Management of Third-Party Provider Relationships Completed During 2019 and 2020

For the one ongoing monitoring activity to monitor and evaluate Fannie Mae's development and implementation of a TPRM framework that was planned and completed during 2019 and 2020, we found that DER complied with its Ongoing Monitoring Examination Processes and Documentation OPB. Based on our review of the examination workpapers for this activity, we determined:

- The initial procedures documents included an examination objective that was consistent with the objective in the approved examination plan, detailed work steps

[8] In support of this argument, DER referenced a recently issued (December 2020) OPB titled Monitoring which included, as a new type of examination activity, "enhanced risk monitoring." Whatever the future merits of "enhanced risk monitoring," that OPB is only effective for the examination cycle beginning January 1, 2021, which is outside the scope of this audit. Accordingly, this OPB has no application to the supervisory activities planned and completed during the years 2014 through 2020.

that addressed the examination objective; the initial procedures documents were approved by the Examiner-in-Charge (EIC).

- The completed procedures documents contained work steps that were consistent with those in the initial procedures document and documented the results of the examiner analysis; the completed procedures documents were approved by the EIC.

- The analysis memoranda documented conclusions that were consistent with the examiner analysis in the completed procedures document; the analysis memoranda were approved by the EIC.

FHFA Followed its Standards in its Performance of Ongoing Monitoring – Remediation Activities for MRAs Related to Fannie Mae's Management of Third- Party Provider Relationships

DER completed three ongoing monitoring – remediation activities to assess Fannie Mae's remediation of MRAs relating to the TPRM framework; one in 2019 and two in 2020. Our review of examination workpapers for each ongoing monitoring – remediation activity found that DER examiners met applicable guidance in the conduct of these activities. In each activity, DER examiners assessed the adequacy of the affected Enterprise's efforts to implement its approved remedial plan.

- Ongoing monitoring – remediation of a 2017 MRA regarding [redacted]. Our review of the workpapers found that DER examiners reviewed and approved Fannie Mae's proposed remediation plan which contained three elements, and assessed the adequacy of implementation of each element. DER closed the MRA in June 2019.

- Ongoing monitoring – remediation of a 2017 MRA regarding [redacted]. Our review of the workpapers found that DER examiners reviewed and approved Fannie Mae's proposed remediation plan and assessed the efficacy of the implementation, as it proceeded. DER closed the MRA in February 2020.

- Ongoing monitoring – remediation of a 2013 MRA based on a deficiency in Fannie Mae's [redacted], which was identified during DER's 2013 targeted examination of Fannie Mae's vendor risk management. While DER examiners reviewed and approved a proposed remediation plan in January 2014, our review of workpapers found that Fannie Mae did not remediate the deficiencies underlying the MRA and DER kept the MRA open. After seven years of remedial efforts by Fannie Mae, DER determined

that Fannie Mae had addressed the deficiencies that gave rise to the 2013 MRA and closed it in February 2020.

FINDING

- DER did not complete any targeted examinations of Fannie Mae's TPRM program, an area of acknowledged [redacted]-risk, from 2014 through 2020.

CONCLUSION

DER's completed examination activities related to Fannie Mae's TPRM program, an area of known [redacted] risk, consisted solely of ongoing monitoring activities from 2014 through 2020. The supervisory framework in effect for these examination activities called for ongoing monitoring to be used to analyze information and identify Enterprise practices and changes in an Enterprise's risk profile that may warrant supervisory attention. Under this supervisory framework, targeted examinations complement ongoing monitoring and enable examiners to conduct "a deep or comprehensive assessment" of selected areas found to be of high importance or risk.

DER records show that DER's last completed targeted examination of Fannie Mae's TPRM program was during the 2013 examination cycle. DER issued [redacted] MRAs from this targeted examination; for [redacted] of those MRAs, Fannie Mae took more than six years to address the deficiency that gave rise to it. In light of the express recognition by DER and Fannie Mae of the established [redacted] risk associated with management of these third party providers and the more than six years that Fannie Mae took to remediate the [redacted] MRA, the governing supervisory framework warranted the completion of one or more targeted examinations of this risk in the years 2014 through 2020. No targeted examinations were completed during this period.

For 2019 through December 31, 2020, DER planned and completed only one ongoing monitoring activity for Fannie Mae's TPRM program, a known high risk to Fannie Mae.

The one ongoing monitoring activity and three MRA remediation activities related to Fannie Mae's TPRM program that DER completed during 2019 and 2020 complied with applicable examination guidance.

RECOMMENDATION

We recommend that FHFA:

1. Ensure that DER uses its full range of available examination activities, including targeted examinations and when appropriate, enhanced risk monitoring, to provide comprehensive assessments of known areas of high risk, like Fannie Mae's reliance on third-party vendors.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA with an opportunity to respond to a draft of this audit report. FHFA provided technical comments on the draft report and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix of this report. In its management response, FHFA agreed with the recommendation and stated that DER is planning to conduct a targeted examination of Fannie Mae's information technology third-party oversight during the 2021 examination cycle. DER is also planning to review and update its internal supervisory guidance on the examination planning process. According to DER, this update will provide more detailed guidance to the EICs and examination managers for developing the examination plans, including factors (e.g., the nature of the objective and/or scope of the supervisory activity, the extent of change in the area at the Enterprise) to be considered when determining the types of supervisory activities that should be included on the examination plans. DER then plans to begin to conduct post-hoc quality control reviews of the examination plans. The first quality control review will be conducted for the 2022 examination plans and will be available by March 31, 2022.

We consider FHFA's planned corrective actions responsive to our recommendation.

In its management response, FHFA also acknowledged that it last completed a targeted examination of Fannie Mae's vendor management process in 2013 but noted that that DER had regularly and comprehensively reviewed Fannie Mae's TPRM framework through ongoing monitoring and issued adverse examination findings. FHFA contended that the fact that the examination activities were classified as ongoing monitoring had absolutely no bearing on the comprehensiveness of the work performed and/or documentation of the work.

We maintain our position that, given the known [redacted] risk associated with third-party provider relationships and the more than six years that Fannie Mae took to remediate the 2013 MRA on [redacted], application of DER's supervisory framework should have caused DER to schedule and conduct targeted

examinations of Fannie Mae's TPRM program to provide "deep or comprehensive assessment[s]," along with ongoing monitoring.

OBJECTIVE, SCOPE, AND METHODOLOGY

We conducted this audit to determine what examination activities DER completed, during the period 2014 through December 31, 2020, in response to identified risks in Fannie Mae's management of third-party provider relationships with vendors that provide operational support and information technology services, such as vendors that supply products, information, and services (e.g., audit and accounting services, telecommunications, data, cloud computing, information security).[9] We also assessed in this audit whether FHFA followed its standards when performing the ongoing monitoring activity (and three ongoing monitoring activities to assess the sufficiency of MRA remediation), which were completed during 2019 and 2020.

We performed the following to accomplish our objective.

- Reviewed the relevant guidance:
  - FHFA Examination Manual (Dec. 2013)
  - AB 2018-08, *Oversight of Third-Party Provider Relationships* (Sep. 2018)
  - OPB, Examination Processes and Documentation: Ongoing Monitoring (Dec. 11, 2018; administratively reissued Feb. 24, 2020)
  - OPB, Examination Processes and Documentation: Issuance of Adverse Examination Findings and Assessment of MRA Remediation (Oct. 31, 2018; administratively reissued Feb. 24, 2020)
  - OPB, Independent Quality Control Process (Jan. 23, 2018; administratively reissued Feb. 24, 2020)
  - Third-party Relationship Management, Draft Supplemental Examination Guidance (2013)

[9] Both Enterprises rely on seller/servicers, including nonbank seller/servicers, which are also third-party provider relationships. Those relationships, however, are managed according to Enterprise selling and servicing guides. DER's rating of risk in third-party provider relationships is driven, in part, by the volume and complexity of Enterprise relationships with seller/servicers. FHFA's oversight of Enterprise supervision over seller/servicers is not included in the scope of this audit.

- Oversight of Third-Party Provider Relationships, Enterprise Examination (Mar. 2020)
- GAO-14-704G, *Standards of Internal Control in the Federal Government* (Green Book)

- Interviewed DER officials to gain an understanding of DER's policies, procedures, modules, and examination practices related to third-party provider relationships.
- Inquired of FHFA officials whether Division of Resolutions performed oversight of the Enterprises' compliance with AB 2018-08.[10]
- We compared FHFA's draft supplemental guidance (field test), Third-party Relationship Management (2013) and the Enterprise Examination Manual module, Oversight of Third-Party Provider Relationships (2020) to the supervisory expectations detailed in AB 2018-08 to determine whether the modules are consistent with these supervisory expectations and sufficient in scope to serve as a resource and reference for DER examiners to understand, evaluate, and assess risks associated with the Enterprises' third-party provider relationships.
- Reviewed FHFA's examination plans for the period 2013 to 2018 for Fannie Mae and identified examination activities related to the management of third-party provider relationships that provide operational support and information technology services.
- Reviewed FHFA's examination plans for 2019 and 2020 for Fannie Mae to determine the population of examination activities related to the management of third-party provider relationships that provide operational support and information technology services. We excluded examination activities focused on sellers and servicers. We confirmed with DER that it performed one ongoing monitoring and three ongoing monitoring for MRA remediations examination activities related to the management of third-party provider relationships. In addition, DER planned and began another ongoing monitoring and a targeted examination, however, these examination activities were not completed as of the end of 2020.
    - For the one ongoing monitoring activity that was completed, we obtained and analyzed the initial procedure documents, completed procedure documents and

[10] These officials explained that Division of Resolutions has not nor would be expected to perform oversight of the Enterprises' compliance with AB 2018-08. They further explained that DER's Office of Risk and Policy was responsible for drafting, fielding comments from the Enterprises, and issuing the Advisory Bulletin. After issuance, questions regarding compliance would have been fielded by DER.

analysis memorandum, and tested the documents for compliance with DER's OPB, Examination Processes and Documentation: Ongoing Monitoring.

- For each of the three ongoing monitoring remediation activities, we obtained the analysis memorandum and remediation letter and tested for compliance with DER's OPB, Examination Processes and Documentation: Issuance of Adverse Examination Findings and Assessment of MRA Remediation.

- For each of the three ongoing monitoring remediation activities, we obtained the Quality Control Review Results Reports and tested for compliance with DER's OPB, Independent Quality Control Process.

We conducted this performance audit from October 2020 through March 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Marla A. Freedman, Senior Audit Executive, Office of Inspector General (OIG)

FROM: Paul J. Miller, Deputy Director, Division of Enterprise Regulation (DER)

SUBJECT: Draft Audit Report: *Despite FHFA's Acknowledgement that Enterprise Reliance on Third-Parties Represents a Significant Operational Risk, It Completed No Targeted Examinations of Fannie Mae's Third-Party Risk Management Program Over a Seven Year Period*

DATE: March 24, 2021

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) draft report referenced above (Report). While FHFA acknowledges that it last completed a targeted examination of Fannie Mae's vendor management process in 2013, we have regularly and comprehensively reviewed Fannie Mae's third-party risk management (TPRM) framework through ongoing monitoring and issued adverse examination findings. Given the significant and ongoing level of change that was taking place as Fannie Mae implemented a new TPRM framework to address DER's concerns, DER followed a strategic approach and utilized ongoing monitoring over targeted examinations. The fact that the examination activities were classified as ongoing monitoring had absolutely no bearing on the comprehensiveness of the work performed and/or documentation of the work. The draft Report makes one recommendation:

Recommendation 1: *OIG recommends that FHFA ensure that DER uses its full range of available examination activities, including targeted examinations and when appropriate, enhanced risk monitoring, to provide comprehensive assessments of known areas of high risk, like Fannie Mae's reliance on third-party vendors.*

Management Response: FHFA agrees with the OIG's recommendation. DER is planning to conduct a targeted examination of Fannie Mae's information technology third-party oversight during the 2021 examination cycle. DER is also planning to review and update its internal supervisory guidance on the examination planning process. This update will provide more detailed guidance to the Examiners-in-Charge and examination managers for developing the

examination plans, including factors (e.g., the nature of the objective and/or scope of the supervisory activity, the extent of change in the area at the Enterprise) to be considered when determining the types of supervisory activities that should be included on the examination plans. DER will then begin to conduct post-hoc quality control reviews of the examination plans. The first quality control review will be conducted for the 2022 examination plans and will be available by March 31, 2022.

We would like to thank the OIG staff that worked with the Agency during this audit. If you have any questions related to our response, please do not hesitate to contact Eric Wilson.

cc: Chris Bosland
Kate Fulton
Scott Valentin
Eric Wilson
John Major

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219